

The “Not Top 10” Trends in Cybersecurity

Public Sector Cybersecurity Trends Continue to Challenge

Bob Smock

Vice President, Gartner Consulting Security & Risk Management

Being busy is most often
used as a guise for avoiding
the few critically important
but uncomfortable actions.

Timothy Ferriss

Fear, Uncertainty, and Doubt [FUD]

KB Financial Group (S. Korea), NongHyup Card and Lotte Card, 104,000,000 records exposed; insider data theft; unknown remediation cost

Healthcare accounted for the most number of incidents AND number of records exposed; Government was 2nd; Retail 3rd

NongHyup Life Insurance (S Korea), 350,000 records exposed via 3rd-party exposure; unknown remediation cost

20 Iranian banks, 3M records exposed via insider "hactivism"; unknown remediation costs

Neiman Marcus revealed more than 1.1 million customers were affected in a hack that occurred over 6 months before discovery. Additionally, 2,400 payment cards were subsequently used fraudulently.

US OMB breach exposes personal info of 19.7M federal applicants plus 1.8M relatives and other associates including 3.6M of current and former employees

Citigroup, 360,000 records exposed via 1) system configuration breach, 2) process exposure; government lawsuit limits release of details

Fraud accounted for 21% of exposed records, but was just 2% of incidents. A single act of Fraud exposed 104M records.

Heartland Payments Systems, 134M records exposed via malware injection on weak applications; \$140M in remediation costs

Morningstar Investments, 184,000 records exposed; refused to release scope or cost of document repository breach

South Carolina had 3 major breaches in four months including the Department of Revenue data exposure: 3.8m SSNs, 650k business tax filings; 400k credit/debit card numbers; \$340M in remediation costs

Target was breached for 40 million customer accounts including encrypted PIN numbers, credit and debit card numbers, card expiration dates, and the embedded code on the magnetic strip on the back of cards.

9 Standard threat patterns: 1) miscellaneous human/configuration errors 2) Crime-ware (malware) 3) Insider/privilege misuse 4) Physical theft/loss 5) Web app attacks 6) Denial-of-Service attacks 7) Cyberespionage 8) Point-of-Sale intrusions 9) Data-theft via Card skimmers
83% of incidents involve the 1st 3

Sony exposed customers' personal and credit card information affecting 77 million people.

Epsilon, the world's largest permission-based email marketing service, announced data breach that affected over 108 retail stores, major financial firms and non-profit organizations.

TotalBank (S Florida), 72,500 records exposed; refused to release data exposure details

Adobe hackers obtained personal and financial data for almost 150 million customers. It was later discovered that the hackers had posted the personal data online.

State of Utah Department of Health: 780k individuals personally identifiable information stolen/hacked; 3rd-party contractor lost thumb drive containing information for 6k Medicaid recipients; \$10M in remediation costs

During the previous 18 months, 3 incidents secured a place on Top 10 All Time List.

Defibrillator - A research team compromised an implanted defibrillator by reverse engineering the wireless communication protocol and controlling it. They were able to change therapies, including disabling the device -- and this is with a real, commercial, off-the-shelf device -- simply by performing reverse engineering and sending wireless signals to it.

Zappos breach exposed the names, addresses, phone numbers, partial credit card numbers, and email addresses of 24 million customers

Officially, 429M personal records were exposed but this is regarded as under-reported with an 85% jump in number of organizations refusing to report size & scope

Texas Comptroller data exposure of 3.5 million records (name, address, SSN, DOB) as part of compiled data from other agencies posted on publicly accessible site, exposed for 18 months prior to discovery; \$5M in agency remediation costs

White Lodging Services experienced a data breach that occurred at its properties including Marriott, Radisson, Renaissance, Sheraton, Westin and Holiday Inn franchises around the country.

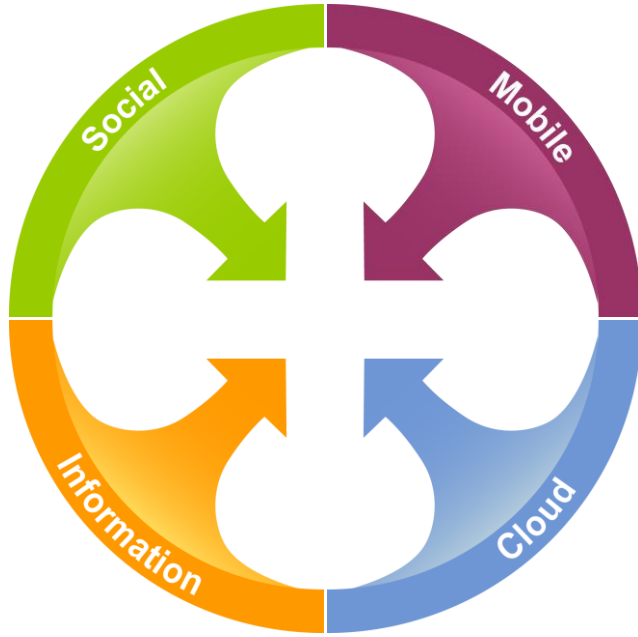
9 "mega-breaches" of personal data last year with more than 2500 security incidents overall, exposing more than 1B records

Two-thirds of incidents exposed between 1 and 1000 records; however, 10 incidents exposed more than 1M records each.

Global Payments Inc., 5.5M records exposed via malware injection; \$94M in remediation costs

California Department of HealthCare Services; 14,000 Social Security Numbers posted to website; 4 exposures in 6 months; \$5M in remediation costs

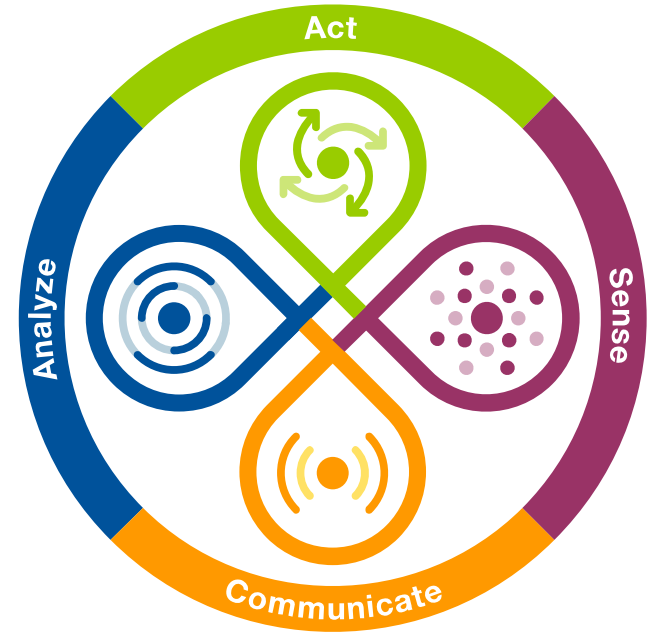
It's not your parent's business world anymore!



Nexus of Forces




Digital Business





Internet of Things


Social/Political Unrest – Economic Disruption – War/Terrorism


And it's not your parent's business risk anymore either!


 **Reputation****
“It takes 20 years to build a reputation and 5 minutes to ruin it” – *Warren Buffet*


 **Cyber Liability****
“Determined attackers can get in. They can cause damage. Can the business or services keep going!” – *GCHQ Director R. Hannigan*


 **Supply Chain***
“Recent catastrophes point to the need to build resiliency into supply chains as a business priority” – *AIG*

 **HR Related Risks***
“Every economy's ability to compete depends on a steady supply of human capital and talent” – *Boston Consulting*


 **IP Theft****
“Picasso had a saying: “Good artists copy; great artists steal” and we have always been shameless about stealing great ideas” – *Steve Jobs*

 **Climate Change**
“There is no one better able to help the world manage its risks than the insurance and reinsurance industry” – *UN Executive Secretary Christina Figures*

 **Catastrophe Risk***
“Total economic losses from catastrophes in 2015 reached \$85 billion. Of this total approximately \$32 billion was covered by insurance” – *Swiss Re Sigma*

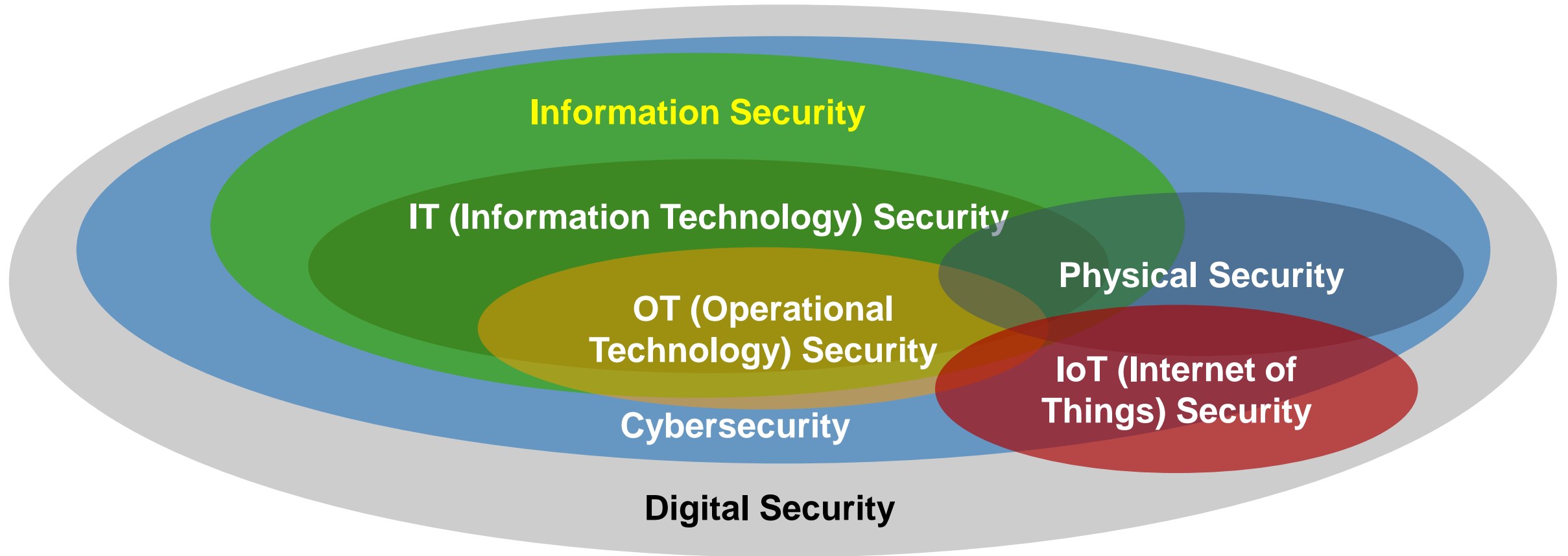
 **Political Risk**
“25 years after the fall of the Berlin Wall, the world again faces the risk of major conflict between states” – *WEF lead economist M. Drzeniek-Hanouz*

 **Mass Migration & Social Upheaval**
“If Europe fails on the questions of refugees, then it won't be the Europe we wished for” – *Angela Merkel*

 **Internet of Things****
“Autonomy will also open up ways for a car to be more of a potential lethal weapon than it is today” – *U.S. FBI*

By 2020, 60% of digital businesses will suffer major service failures due to the inability of IT security teams to manage digital risk.

And the universe of security has changed as well.



By 2020, at least one major safety incident will be caused by an IT security failure, leading to significant injury...and new regulation

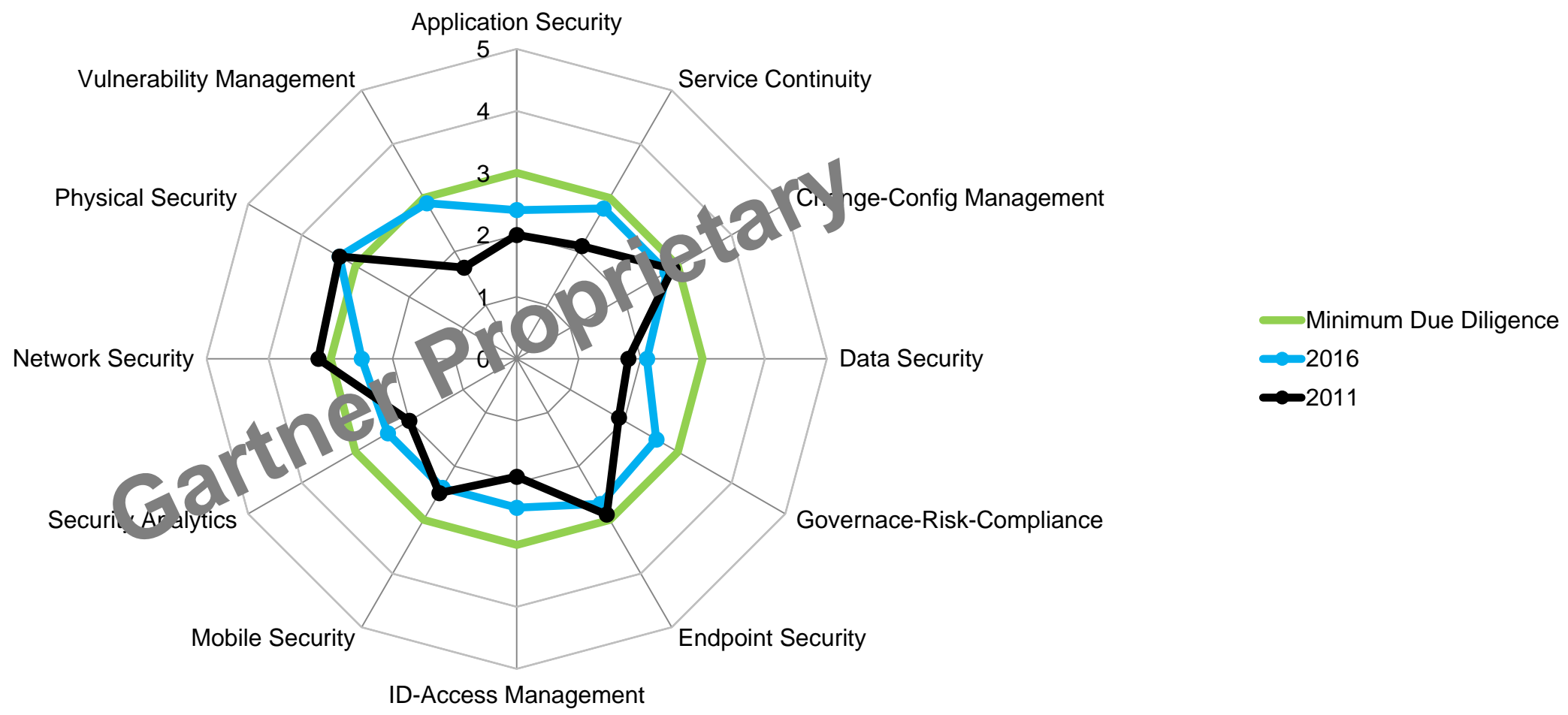
Endeavor to Persevere

The concept of security is simple.

But executing security in this day and age is a journey for which there are no shortcuts.

- *It's goes beyond simply being about technology.*
- *It's expensive and requires continuous investment.*
- *It takes time and requires constant attention.*
- *It forms complex relationships and is part of everything you do.*
- *And the need for it never ends.*

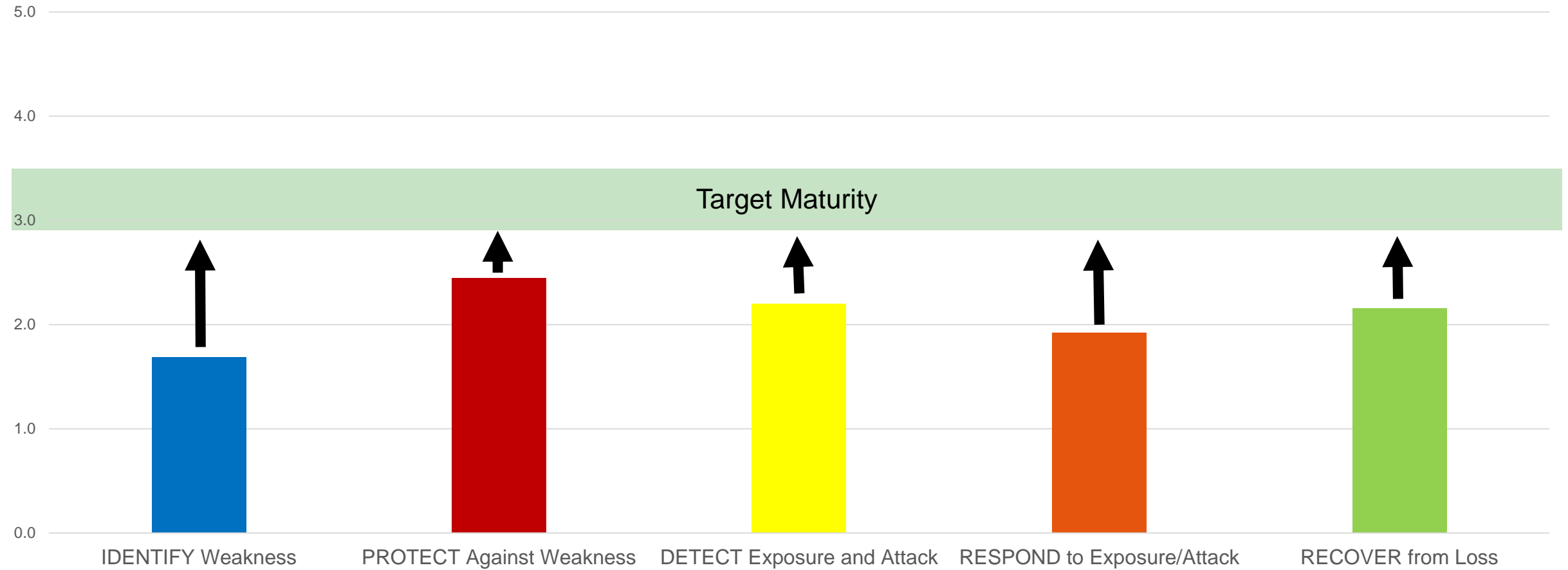
Security Maturity through the decade so far...



“By 2020, organizations that are below maturity Level 3 in their InfoSec program will have increased judicial, legislative, and regulatory liability over those at Level 3 and above”

Translation...

Functions of the NIST Cyber Security Framework



“By 2020, organizations that are below maturity Level 3 in their InfoSec program will have increased judicial, legislative, and regulatory liability over those at Level 3 and above”

#10 – [Tie] Change Impact and PKI Management: 89%

1. Cross-function/process view of impacts to security posture

Formal change management security “gate”

2. Certificate Authority (CA) operational integrity

CA governance and procedural enforcement

Ability to provide expected or required level of protection

Data, access, or system/application

#9 – Internal Network Transmission Protection: 90%

System-to-System communication

The “soft, chewy” inside

Application-based vs. Network-based

Keep it simple

Ability to provide expected or required level of protection

Data exposure and leakage

#8 – Hardcopy Data Protection: 91%

Most overlooked aspect of data protection

Health services, Government, Retail are top 3

Policy and protection per Use Case

Use, Storage, Retention, Destruction

Ability to provide expected or required level of protection

Data exposure and leakage

#7 – [Tie] Environment Validation and Event Management: 93%

1. Infrastructure configuration integrity

Alert on change or periodic scan vs. CMDB

2. Security Information and Event Management

The lynchpin of comprehensive and accurate detection

Ability to provide expected or required level of risk mitigation

Reactive Posture

#6 – Insufficient Security Resources: 94%

Lack of numbers

Skills, knowledge, experience, “passion”

Primary cause for the failure of security governance

If security governance doesn't work – security doesn't work

Ability to provide expected level of risk management & mitigation

Unmanaged residual risk

#5 – Identity and Access Management Strategy: 95%

Identity & Access Lifecycle

From vetting through archive including provisioning & reporting

Use cases include sources, targets, and user experience

Got automation for enforcement, consistency, and cost-efficiency?

Ability to provide expected level of policy enforcement

Don't forget about IAM-specific governance

#4 – Mobile Data Protection: 96%

2nd-most overlooked aspect of data protection

“Removable” media

Use-case enforcement

Endpoint enforcement, device whitelist, DLP

Ability of users to provide expected level of protection

Protect the data itself

#3 – Business Impact Assessment: 97%

Prioritization of resources

Business mission critical

“Business” vetted

Cost vs. Reality

Ability to meet expected level of service restoration

Extended service and data outage

#2 – Secure Application Coding Practices: 98%

Coding practices and enforcement frameworks

programming methods, techniques and standards

Code assurance and testing

Functional vs. security assurance

Ability to provide expected level of protection

Transaction confidence

#1 – [Tie] Vulnerability Remediation and Database Protection: 99%

1. Comprehensive program of vulnerability scan & Pen Test

Internal, external, 3rd-party, app & infrastructure, pre-production

2. Field-level sensitive data encryption

1st rule of security: Protect the data itself

Ability to provide expected level of risk management & mitigation

Reactive or dependent posture to exploitation and data leakage

Identify Protect

Gartner

Honorable Mention: 82%

1. Data Classification

Policy to define types, protections, use cases; identify & enforce

2. Multi-factor authentication for risky use cases

Remote, privileged, and critical data access

3. Formally defined security program across business units

Security Management Plan

Call to Action

Next Week

- ✓ Enjoy the Easter break!

Next Month

- ✓ Review your strategy roadmap/POAM and evaluate the need for change

Next Quarter

- ✓ Do what you can. Get help where you need it. Outsource if it makes sense.
Acknowledge the risk of what's not done.

| | |
|---|----|
| Database Protection | 1 |
| Proactive Vulnerability Remediation Program | 1 |
| Secure Coding Practices | 2 |
| Business Impact Assessment | 3 |
| Mobile Data Protection | 4 |
| IAM Strategy | 5 |
| Insufficient Resources | 6 |
| Environment Configuration Validation | 7 |
| Security Information & Event Management | 7 |
| Hardcopy Data Protection | 8 |
| Internal Network Transmission Protection | 9 |
| Security Impact Evaluation | 10 |
| PKI Management | 10 |
| Multi-Factor Authentication | HM |
| Data Classification Policy | HM |
| Security Management Plan | HM |

Computers at Risk, National Research Council, 1990

“Organizations have a duty to preserve and protect assets and constituents, and to maintain the quality of service.

To this end, management must assure that operations are carried out *prudently* in the face of *realistic* risks arising from *credible* threats.”

Avoid doing security simply for the sake of doing security